State Information Technology Advisory Committee

December 9, 2013
1:00 PM – 3:00 PM
Brynhild Haugland Room

Members Present:
Mike Ressler – Chair, Darren Brostrom, Eric Hardmeyer, Alvin A. Jaeger, Bryan Klipfel, Grant Levi, Representative Mark Owens, Senator Larry Robinson, Sheila Peterson for Pam Sharp, Arvy Smith, and Cher Thomas for Tom Trenbeath

Members Absent: Peggy Link, Maggie Anderson, Sally Holewa, Cory Fong, Lisa Feldner and Sparb Collins

Others Present:
Jeff Quast, Dan Sipes, Doran Eberle, Duane Schell, Gary Vetter, Mark Molesworth, Justin Data, Dirk Huggett, Dave Eckenrode and Tim Schenfisch

Scribe:
Jeff Quast

Mr. Ressler called the meeting to order at 1:08 PM, a quorum was present

Agenda / Topics discussed

Welcome – Mike Ressler

- Mr. Ressler reviewed the agenda and welcomed the participants

EA Waivers and Standards – Jeff Quast

- Mr. Quast gave an overview of EA activities since the last SITAC meeting

Application Security – Dan Sipes

- Mr. Sipes explained AppScan and what it does
- Starting by scanning applications developed by ITD
- ITD will then begin scanning applications for other agencies developed by external vendors
- If a high risk vulnerability is found ITD will escalate the issue to secure the app and data
- Also paired with ManTech security audit
- Mr. Hardmeyer asked if this is like SAS70
    - Mr. Sipes answered that we are working with the Auditor's Office to make it more regularly scheduled, perhaps every 2 years
- Senator Robinson asked if AppScan is new and how sophisticated is it, and what are other states are doing
    - Mr. Sipes answered the tool is not new, it is one of many, in this case from IBM
    - Senator Robinson asked if we are satisfied with the product
    - Dan answered that yes we are, and asked ManTech to also give their opinion

- Senator Robinson asked if ITD and the state has the resources to respond to threats, are we asking for more than what we have resources to
  - Mr. Sipes answered that ITD tries to be proactive and not reactive
  - There are some challenges to stay proactive, and a need to focus on the primary risk areas
  - ITD has made investments at the network level that are blocking a lot of threats
  - Senator Robinson suggested a request for FTEs could be considered if they are needed
- Mr. Klipfel asked if PowerBuilder apps would be included in the scanning process
  - Mr. Sipes answered that .net and Java are the only types of apps that will be scanned
- Mr. Klipfel asked about apps on iPads and other mobile devices and if there was a risk with those apps syncing to the network
  - Mr. Sipes answered that the tools are not as robust as on pcs
  - Also be aware of what data is being stored on the device, and that you can use mobile device management tools to help control and secure the device
- Mr. Brostrom asked that in situations where an agency has a vendor provided product, does ITD work with the vendor or the agency
  - Mr. Sipes answered that ITD would begin the process with the agency, then may have to include the vendor depending on the results. ITD would not expect the agency to then work with the vendor alone, it would be a collective process between the agency and ITD
- Mr. Brostrom asked what the situation would be if the vendor hosted the app
  - Mr. Sipes answered ITD can't scan those, but could ask the vendor to scan it or could contract with someone like ManTech to do it, which would incur a cost
  - Ms. Thomas added that it may be something we should be including in software development contracts

Security Breach Process – Mike Ressler
- Mr. Ressler explained that ITD is not trying to sound like an alarmist, but is focusing on security
- The tools the bad guys are using are becoming more sophisticated
- It is not if but when we have some level of breach, which is not ITD giving up
- In the event of a breach, it is important for agencies to have a plan to address a breach
- The first thing an agency should do is contact ITD
- The first step is to determine if your agency has PII and which applications have access to it
- The first phone call from ITD will be to the department head of the agency
- The next step would be to contact AG office, then Tag Anderson, then the Governor's Office
- Mr. Ressler answered an earlier question from Senator Robinson, that ITD intends to put a budget request package together for next biennium to address specific security resources
- Senator Robinson again asked if ITD is maxed out on resources, or approaching that
  - Mr. Ressler answered that ITD is approaching that quickly

Disaster Recovery – Dan Sipes
- Mr. Sipes explained that business continuity is a responsibility not just for ITD but all agencies
- Agencies should be thinking about business continuity and have a thorough plan
- Two main points to consider in IT
  - Recovery point objective = point in time you are OK with going back to
  - Recovery time objective = how long can I take to get back up to speed
- ITD has service level agreements to define enterprise service continuity levels
- Mr. Sipes covered which current services have priority
- You can't get better disaster recovery without an investment
- Testing disaster recovery once it is established is also a cost and requires agency investment
- Mr. Jaeger commented that with the phones connected to the computer system, it is concerning that they could go down.
  - Mr. Sipes commented that the core phone system is highly available, but the "last mile" connection is always going to be the weak link

o Agencies must also decide how important every service, including phones, are to their business processes
o For agencies in the capital, some of the conversations may need to be with facilities management

FirstNet – Duane Schell
- Mr. Schell gave some background on the initiative
  - First Responders Network Authority
  - Received Wireless Spectrum – license to use a certain amount of the wireless network
- Intent is to build a nationwide wireless 4g network
  - Should be more reliable than a commercial network
  - Commercial networks have proven to be very troublesome in emergencies
- ND awarded $1.1M
  - Will be difficult to get 100% coverage
- Joint effort between ITD and DES
- ND will be able to opt in to a federal model, or opt out and build our own
- Senator Robinson asked if there will be ongoing costs
  - Mr. Schell answered yes, it will likely be a fee for service model
- Representative Owens asked who exactly is FirstNet Authority, and do we have a seat at the table
  - Mr. Schell answered they are a board
  - ND's voice is through a number of organizations that we are involved in
- Mr. Levi asked what legal obligations are driving the choice to opt in or opt out, and can we do nothing
  - Mr. Schell answered that doing nothing is the same as opting in
- The costs in many cases are already incurred with private companies, hopefully FirstNet will be competitive, so the cost would just shift
- Senator Robinson asked what the rollout schedule is
  - Mr. Schell answered that the project is behind schedule, 2015 at the earliest
- Representative Owens mentioned that it will be a lot of work and asked if they will be kept up to speed on the progress and details
  - Mr. Schell answered yes, we are beginning state meetings this week and will be developing requirements
- Mr. Ressler added that the governors in each state are ultimately responsible for ensuring it is covered
- Very likely existing carriers will be providing the network

Business Analysis – Mike Ressler
- Mr. Ressler expects Business Analysis to have the same impact on success as Project Management has had
- Business Analysis should precede the budget request / cost estimating / RFP
- Quite a few people have been trained in BA already
- Mr. Levi mentioned that more often now that they are buying COTS products and fitting their business model to the products, and asked if BA can be incorporated into that model
  - Mr. Ressler answered that it will help by documenting processes before getting the products, and can then more easily pick the proper vendor or product and deal with gaps
- Senator Robinson mentioned that we seem to be constantly improving, and maybe our expectations are not always realistic, and asked if would it be better to break down a project into a series of benchmarks
  - Mr. Ressler answered that it would help, and it is difficult to do long, large projects with accurate cost estimates
  - Ms. Thomas added that it is really helpful to define business processes separately and accurately so you can prioritize efforts

- Senator Robinson pointed out that scope changes and costs are not just part of IT project, they are seeing it in all kinds of projects in the state

Secretary of State Project – Al Jaeger / Mike Ressler
- Mr. Molesworth gave an overview of the large project oversight process and purpose of variance reporting, which is over 20% for schedule or budget
- The purpose is to share lessons learned to help future projects be more successful
- Mr. Ressler explained the causal factors
  - Expected to be able to use existing code from another vendor
  - Business processes were more complex than expected
  - Business Analysis process had some struggles
  - Staffing resources were limiting
- Mr. Jaeger added that they started with 5 months of requirements gathering
- Mr. Ressler added that part of the problem may be that developers doing requirements gathering is not the same as business analysts doing it
- Lessons learned
  - We seldom staff up adequately for large projects
- Secretary of State workloads increased by huge margins in the last 3 years
- Recovery Strategy
  - Re-plan is being developed for early 2014
- Senator Robinson pointed out that we are still improving and learning, and it is important to be transparent

WSI Project – Clare Carlson
- Mr. Molesworth explained that this project report is close out
- Mr. Carlson explained that the project was terminated
- Causal Factors
  - Vendor did not perform
  - Multiple changes in WSI executive leadership
  - Project led to morale issues and burn out
- Lessons Learned
  - Mange vendor contracts to the letter
  - Require full-time onsite personnel
  - Use a PMP credentialed project manager
  - Invest in business process modeling
  - Formulate an Organizational Change management strategy
  - Executives need to be transparent and involved
  - Allow additional lead-time for resource needs
  - Avoid significant modifications to COTS products
- Mr. Hardmeyer asked what the plan is now
  - Mr. Carlson answered they are using the existing system
- Mr. Hardmeyer added that when they were building a system from scratch, they overbuilt due to requests from employees wanting the system to be perfect, and also ran into problems with employees trying to do their regular jobs and take on new projects
- Mr. Jaeger pointed out that many of the lessons learned were similar to the SoS project

Wrap-up

Future Topics/ Closing Comments – Mike Ressler
Mr. Ressler thanked the committee members and other attendees and encouraged everyone to contact him with ideas for future topics

Mr. Levi suggested that we spend some time reviewing successful projects and what does work well at a future meeting

Adjournment – Mike Ressler

- Mr. Ressler adjourned the meeting at 3:30 PM